UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/598,218 | 08/21/2006 | Steve Bae | 2060-01 | 1338 |

52706 7590 05/04/2009

IPLA P.A.
3580 WILSHIRE BLVD.
17TH FLOOR
LOS ANGELES, CA 90010

| EXAMINER |
|---|
| VAUGHAN, MICHAEL R |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2431 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 05/04/2009 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/598,218 | BAE ET AL. | |
| | Examiner | Art Unit | |
| | MICHAEL R. VAUGHAN | 2431 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *11 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-6* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

The instant application having Application No. 10/598218 is presented for examination by the examiner. Claims 1-6 are pending. Claims 1-5 have been amended.

## *Response to Amendment*

### *Claim Objections*

Present amendment overcomes the previous claim objections.

### *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 5 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 5, Examiner is interpreting this claim to provide the functionality that denies authorized application from writing in disk drive area. As such, the single condition of determining if the function is a write operation is insufficient. The specification says (and claim 1), that authorized applications are permitted to write in the VSD area. Therefore claim 5 would contradict that teaching as claimed because all

authorized application would be prohibited from writing. It appears that in addition to the write condition, there needs to be the condition of disk drive access. Therefore, if function is a write operation **in the disk drive**, and it is determined that the application module has been authorized, the operation would be stopped. And similarly, if the function is a write operation **in the disk drive**, and it is determined that the application module has been unauthorized, the operation would be permitted. This would allow authorized programs to write in the disk drive. Also the phrase "the function is a function" is indefinite because it unclear if there are two functions or just one. The phrase "if the function is requesting" conveys the same meaning without the indefiniteness. Claim 6 is rejected for being dependent on claim 5.

## *Response to Arguments*

Applicant's arguments with respect to claims 1 and 4 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2002/0099944 to Bowlin in view of USP Application Publication 2003/0159070 to Mayer et al., hereinafter Mayer.

As per claim 1, Bowlin teaches an access control system, comprising:

a Virtual Secure Disk (VSD) image file module [virtual directory] occupying a certain space of a hard disk in a file form (0039);

a VSD drive [safe zone] for processing security-sensitive files within the VSD image file module (0039);

a VSD file system module for allowing an operating system to recognize the VSD drive as a separate disk volume at a time of access (0039) to the security-sensitive files within the VSD image file module (0040); and

an access control module [filter] for determining access by determining whether an access location is a disk drive or the VSD drive (0035) and the application module has been authorized to access a file, which is stored on the hard disk [not in safe zone], to perform tasks in the application module (0040)

wherein an authorized application module is configured to access the VSD drive for write and read operations [0043 and 0045; application are given permissions to files in the safe zone],

wherein an unauthorized application module is configured to access the disk drive for write and read operations [files not in the safe zone are accessible to unauthorized application; 0026], and

wherein the unauthorized application module is not allowed to access the VSD drive (0045 and 0026).

Bowlin is silent in teaches an encryption and decryption module for encrypting and decrypting data input/output between the VSD image file module and the VSD drive and the authorized application module is configured to access the disk drive for a read operation only. Mayer teaches that protected files can be encrypted for certain applications so that only that application may access them (0102, last sentence on page 10). This would take Bowlin system one step further for securing files to specific applications. Bowlin teaches that files in the safe zone (virtual drive) can be given access to specific applications. If then the files were encrypted, this would increase the security of the system. Bowlin teaches encrypting the database which divulges the permissions of the file so encrypting the files is a logical step. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to encrypt the files in the safe zone (virtual drive) because it would further protect those sensitive files. Mayer also teaches the segregating application in to their environment. Specifically Mayer teaches that application should have full access to their own environment but read only access to other share environments [0094; first sentence]. This makes a lot of sense if one considers what would happen if an authorized application is compromised. Preventing a compromised application from copying sensitive

information into a public domain would be catastrophic for an organization. Whether by, malicious intent or accidental, preventing leaking of sensitive data is critical. Modifying the system of Bowlin which this functionality would secure the authorized application from writing the file in the safe zone to an area outside the safe zone. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this teaching into the system of Bowlin for the reasons just mentioned.

As per claim 2, Bowlin teaches wherein the access control module comprises:

an extended system service table [database] for allowing the operation of a corresponding function to be performed when it is pointed at by a descriptor [0035; requesting of an access to a file];

and an extended system table for changing a function, which is requested of the service system table by the application module, to prevent operation of the function, determining whether a space in which a corresponding task is performed is the disk drive or the VSD drive, determining whether access to the corresponding file by the application module has been authorized, and providing the unchanged function to the extended system service table or stopping the operation of the function according to results of the determination [0047]. Bowlin teaches that access attempts within the safe zone by authorized application are denied. Therefore the function is stopped. If it is determined that the function is made by an authorized application to a file in the safe zone it is permitted. Access is based on type of application and where the file resides.

As per claim 3, Bowlin teaches wherein the VSD image file module virtually occupies the hard disk so as to allow the operating system to recognize the data as

being assigned to a certain space of the hard disk without performing physical assignment for storing the data on the hard disk, so that the authorized application module can physically assign the data to the space [virtual directory; 0039].

As per claim 4, Bowlin teaches an access control method, which is performed by an access control system having a hard disk, a disk drive, a file system module [directories in areas not inside the safe zone], an application module [application], a VSD image file module [virtual directory], a VSD drive [safe zone], an encrypting/decrypting module (0046), a VSD file system module [type of file system inside the safe zone], and a control access module [filter] including an extended system service table and an extended service table [databases], wherein the VSD image file module occupies a certain space of the hard disk in a file form [in virtual directories of the safe zone] and the VSD drive for processing security-sensitive files is located within the VSD image file module (0039 and 0035), comprising the steps of:

(a) authorizing the application modules (0045);

(b) the application module calling a function from an operating system to access a corresponding file (0035);

(c) the operating system providing the function to the extended service table (0035);

(e) determining whether of the file is the disk drive or the VSD drive in the extended service table (0041);

(f) providing the original file to the extended system service table if it is determined that the access space is the disk drive at step (e) [file was in unsafe zone so access is permitted; 0035 and 0041];

(g) determining whether the application module has been authorized if it is determined that the access space is the VSD drive at step (e) (0035);

(h) providing the original function to the extended system service table if it is determined that the application module has been authorized at step (g) (0035);

(i) stopping the operation of the corresponding function if it is determined that the application module has not been authorized at step (g) (0035 and 0047).

Bowlin is silent in explicitly teaching changing the function into an arbitrarily designated function to prevent the operation of the function in the extended service table. The tables are interpreted to be equivalent to the database in which the access types and application permissions are stored by which the filter uses to grant/deny access attempts to file stored in the safe zone [virtual drive]. Mayer teaches trapping or hooking a file access type, looking for equivalent function and returning the original function is if the access is authorized (0115). This is one explicit way of performing what Bowlin teaches as not permitting a function access until the filter determines the function and the application are legitimate. It is within the ordinary capabilities of one of ordinary skill in the art to substitute similar known methods which produce predictable results. The trap and return functions of Mayer would not modify Bowlin in an unpredictable way.

As per claim 5, Bowlin teaches if the function is a function requesting a Write operation [access attempt], the step (e) comprises the steps of:

determining whether the application module has been authorized (0035);

stopping the operation of the function if it is determined the application module has been authorized (0035). Bowlin does not explicitly teach the arbitrarily designated function returning to the original function, the operation of which is possible, and being provided to the extended system service table if it is determined that the application module has been unauthorized. Examiner supplies the same rationale for combining Mayer's teaching of hooking and returning the original function as supplied in the rejection of claim 4. Examiner supplies the same rationale for combining Mayer's teaching not permitting authorized application write access to non secure areas of the hard disk as supplied in the rejection of claim 1.

As per claim 6, Bowlin does not explicitly teach the step of the encryption and decryption module encrypting and decrypting data that are input and output between the VSD image file module and the VSD drive. Examiner supplies the same rationale for combining Mayer's teaching of encrypting the file in the safe zone for explicit use by authorized application as recited in the rejection of claim 1.

## ***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/

Supervisory Patent Examiner, Art Unit 2431